REMARKS

Claims 1, 3, 5, 6, 9-11 and 13-19 have been examined.

I. Claim Rejections - 35 U.S.C. § 101

Claims 10, 11 and 13 stand rejected because the claimed invention is allegedly directed to non-statutory subject matter: independent claims 1 and 11 direct to "a detection program", which may comprise only software components as claimed. Therefore, claims 10 and 11 have been amended as suggested by the Examiner. Applicants respectfully request the Examiner to withdraw this rejection in view of the self-explanatory claim amendments made herein.

II. Claim Rejections - 35 U.S.C. § 102

Claims 1, 3, 5, 6, 9-11 and 13-19 stand rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by "SafePatch Version 0.9 User Manual", March 1999 (art made of record, hereafter "the SafePatch Manual"). Applicants traverse this rejection.

A. Claim 1

Claim 1 recites:

> A detection method of omission-in-software-property-management using a network for detecting a computer omitted from a software-property management which manages, for each computer, basic information thereof and installed software, and fix-patch application status, the method comprising the steps of:
>
> performing a first step wherein a network-connected-computer list which holds, for all computers connected to a given network, information for identifying each computer, and a software-property management list which holds, for all computers to be managed by said software-property management, information for identifying each computer, are used as a basis on which a computer is extracted that is present in said network-connected-computer list and absent in said software-property management list; and
>
> performing a second step wherein there is created a list of computer omitted in the software-property management based on the computer extracted that is present in said network-connected-computer list and absent in said software-property management list in the first step,
>
> wherein in the first step, said network-connected-computer list and said software-property management list are used as a basis on which a computer is

> extracted that is present in said software-property management list and absent in said network-connected-computer list, and
>
> in the second step, there is created a list of computer in unused state based on the computer extracted that is present in said software-property management list and absent in said network-connected-computer list.

The SafePatch Manual relates to a management software (SafePatch) which analyzes remote systems to determine the status of security patches and distributes needed patches by performing a job (Introduction). In particular, SafePatch compares the remote system's files with files from patches to determine what is actually installed and what needs to be installed (Introduction). Thus, a Host list is created by a user which designates which computers (i.e., hosts or remote system) to check by performing a job (page 19). The Examiner asserts that the SafePatch Manual discloses each and every feature of claim 1. Applicants respectfully disagree.

The SafePatch Manual discloses that SafePatch is used to analyze remote systems to determine the status of security patches corresponding to other software (e.g., system software of an operating system and patches) (Introduction). Thus, SafePatch is a software-property management software that manages the system software of a remote system (host) (Introduction). However, SafePatch does not generate a list which lists computers in a network that are not being managed by software-property management (i.e., by SafePatch). In addition, SafePatch does not generate a list which lists computers being managed by software-property management (i.e., by SafePatch) that are not connects to the network.

For example, the Examiner asserts that the Figure on page 31 of the SafePatch Manual a network-connected-computer list, which includes all computers connected to a given network. The Figure on page 31, however, is merely a host list, which is a list of remote systems created by a user for which the user may select from to test communications between a Patch Server and the remote system (page 30-31). The SafePatch Manual discloses that a remote system may not be in communication with the Patch Server if (1) the host is not alive or (2) SafePatch is not installed and running (page 31). A host is selected from the host list to test the communication. Thus, the host list is not indicative of whether a host is alive. Firstly, anyone of server 1, server 2 or server 3 provided in the host list may be alive or not alive. Thus, server 1, server 2 and sever 3 are provided in the host list regardless of being connected to a network such that they can be selected by a user for testing communications with the Patch Server. Secondly, anyone of server 1, server 2 or server 3 may be alive, but not running SafePatch. The host list does not differentiate between being alive and not having the management software (SafePatch) installed. Thus, it cannot be said with certainty that every remote system in the host list is connected to a network. For example, SafePatch permits a host to be added to a host list even if SafePatch is not running on the host or the host is not alive (page 4, paragraph 4). Similarly, it cannot be said with certainty that all computers connected to a given network are included in the host list. The SafePatch Manual simply does not disclose a network-connected-computer list which includes all computers connected to a given network.

The Examiner also asserts that page 2 (section 1.1.1.2) and page 34 of the SafePatch Manual disclose holding, for all computers connected to a given network, information for identifying each computer. However, the Examiner fails to recognize that it is the claimed network-connected-computer list which holds the information. The Examiner asserts that the Figure on page 31 of the SafePatch Manual discloses the network-connected-computer list. Page 2 of the SafePatch Manual discloses a step of querying remote systems during an evaluation to determine which patches may be needed. The information obtained from the query not relate to information included in the host list of page 31. Similarly, the Figure on page 34 shows a report of a completed job (pages 33-34). Again, this information does not relate to information provided in the host list of page 31. The Examiner seems to rely on completely different embodiments to disclose this claimed feature. This is entirely improper.

The Examiner asserts that the SafePatch Manual also discloses the claimed software-property management list. The Examiner relies on the Figure of page 1 and pages 17-21 of the SafePatch Manual for disclosing this feature. However, pages 17-21 merely recite a method of making a host list. The method of making the host list results in the completed host list as shown in the Figure on page 31 (i.e., the same list which can be used for testing communications between the patch server). In other words, pages 17-21 disclose selecting remote systems and host groups which can be evaluated **if** the host is alive and **if** the host has SafePatch installed and running (pages 17, 19 and page 31). As stated above, the host list may include remote systems which do not have SafePatch installed and running. Thus, the cited portions of the SafePatch Manual do not appear to disclose a software-property management list...for all computers to be managed by said software-property management.

Also, the host lists disclosed on pages 17-21 does not hold the information the Examiner relies on in page 34 for similar reasons discussed above.

Additionally, pages 17-21 disclose steps for making a host list which results in the list shown in the Figure of page 31 (i.e., a host list). Thus, pages 17-21 and page 31 basically disclose the **same list**. However, the Examiner relies of the host list for disclosing the network-connected-computer list **and** for disclosing the software-property management list (see above). This is impermissible and such double counting **cannot** support the rejection.

The Examiner asserts that the SafePatch Manual discloses using a network-connected-computer list and a software-property management list as a basis to extract a computer that is present in the network-connected-computer list and absent from software-property management list. However, it is not clear how this is possible since the Examiner basically relies on a host list for disclosing both the network-connected-computer list and the software-property management list. Again, a host list is a list of remote computers which can be evaluated by SafePatch (page 19 and page 31). That is, all host lists are based on the same general concept, and can include any number of variations of hosts and host groups (page 19). Furthermore, pages 28-29 of the SafePatch Manual merely disclose how a user creates a Host Group (i.e., a group of remote computes categorized by a same group name) which is added to a host list (pages 19 and 28). Neither the Figure of page 19 nor the Figure of page 31 are used as a basis to extract a computer to a host group. This would not be possible since a host group is merely created based on a user selection (pages 28-29) similar to how a remote system is added to the host list as disclosed on pages 17-21.

More importantly, a host group is not a list of computers omitted (i.e., list of computers extracted) that are present in the network-connected-computer list but absent in the software-property management list. A host group is merely a group of remote systems that are selected to be evaluated by the management software (SafePatch). However, the host group is not by any means indicative computers extracted or of the claimed list of computers omitted, which is a list of the computers extracted. The SafePatch Manual does completely silent about using two lists as a basis for extracting a computer.

Furthermore, the Examiner appears to rely on the report shown on pages 39-40 of the SafePatch Manual for disclosing the list of computers omitted. The report provides details about what patches a remote server needs to install based on an evaluation. However, a patch is not the management software - SafePatch is. That is, a patch is not equivalent to the claimed software property management. A patch is a fix to system software; however, a patch does not manage software property. It is also obvious that any remote system provided in such a report is managed by software property management (i.e., SafePatch), or else SafePatch would not be able to run the report on that remote system. Thus, it should also be clear that the report on pages 39-40 is not a list of computers omitted (i.e., list of computers extracted) that are present in the network-connected-computer list but absent in the software-property management list.

The Examiner asserts that pages 30-31 and 49 of the SafePatch Manual discloses extracting a computer that is present in said software-property management list and absent in said network-connected-computer list. The SafePatch Manual discloses a remote system (host) is selected on an individual basis for testing a communication between the remote system and the patch server (page 31: 2. select a host from the Host List). Thus, the remote system is not extracted based on the presence in said software-property management list and absence in said network-connected-computer list. Instead, the computer is selected by the user for testing. Furthermore, if a communication test fails, the SafePatch Manual instructs a user to troubleshoot by checking whether the selected/tested remote system is alive and that SafePatch is installed and running. The tested remote system could be (1) alive or not alive and/or (2) running SafePatch or not running SafePatch. Page 31 does not differentiate. Instead, it is up to the user to trouble shoot the failed communication. Thus, a window displayed indicating whether the tested remote system passed or failed. However, the "extraction" is based on a user selection of the remote system for testing and not based on whether the computer is present in said software-property management list and absent in said network-connected-computer list.

Furthermore, page 49 (section 7.3) clearly discloses that a message indicating that a host is unreachable is displayed when SafePatch is not detected (i.e., SafePatch is not detected or communicable with because the host is either not alive or because SafePatch is not installed and running on the host (page 31)). Again, the SafePatch Manual does not acknowledge what the root of the problem is, but instead notifies the user via message so that the user can troubleshoot. Thus, the message does not differentiate between a host that is not alive, a host that does not have SafePatch installed, or host that is not alive and that does not have SafePatch installed[1]. The SafePatch Manual simply does not disclose extracting a computer that is present in said software-property management list and absent in said network-connected-computer list. Also, the message in section 7.3 displayed indicating that SafePatch was not detected is not a list of computers in unused state (i.e., list of computers extracted) that are present in the software-property management list and absent in the network-connected-computer list.

In view of the above, the Examiner fails to how the SafePatch Manual discloses each and every feature of claim 1. Applicants submit that the SafePatch Manual fails to disclose the features of claim 1 for at least the above reasons, and thus, claim 1 is patentable.

B. Claims 3, 5, 6, 10 and 11

Claims 3, 5, 6, 10 and 11 include analogous, though not necessarily coextensive features recited in claim 1, and therefore, claims 3, 5, 6, 10 and 11 are patentable for the reasons discussed for claim 1.

C. Claims 14-19

Applicants submit that claims 14-19 are patentable for reasons similar to those presented above in conjunction with claim 1.

[1] For example, SafePatch permits a host to be added to a host list even if SafePatch is not running on the host or the host is not alive (page 4, paragraph 4).

For example, claim 14 recites that the network-connected-computer list is compared with the software-property management list as the basis on which the computer is extracted. The Examiner appears to assert that the Figure on page 34 of the SafePatch Manual is compared to a host list to extract a computer. However, the Figure on page 34 illustrates the results of an evaluation on at least one of the hosts which are selected by a user to be evaluated (page 33-34). Thus, all remote systems selected from a host list to be evaluated by a user are shown in the report on page 34. The SafePatch Manual fails to disclose that any two lists are compared for extracting a computer for creating a list of computer omitted in the software-property management or a list of computer in unused state.

Claim 15 recites that the difference between the network-connected-computer list and the software-property management list is extracted. The Examiner appears to assert that pages 39-40 of the SafePatch Manual discloses the claimed "difference." A list of needed patches, however, does not related to a computer omitted in software-property management. That is because the SafePatch software manages the computers, not the patches. It is clear that any results shown in pages 39-40 related to computers which have SafePatch installed therein.

Claim 16 recites that the computer omitted in software-property management is a computer connected to the network not under software-property management. Again, the Examiner asserts that pages 30-31 and 49 of the SafePatch Manual discloses extracting a computer that is present in said software-property management list and absent in said network-connected-computer list. The SafePatch Manual discloses a remote system (host) is selected on an individual basis for testing a communication between the remote system and the patch server (page 31: 2. select a host from the Host List). Thus, the remote system is not extracted based on the presence in said software-property management list and absence in said network-connected-computer list. Instead, the computer is selected by the user for testing. Furthermore, if a communication test fails, the SafePatch Manual instructs a user to troubleshoot by checking whether the selected/tested remote system is alive and that SafePatch is installed and running. The tested remote system could be (1) alive or not alive and/or (2) running SafePatch or not running SafePatch. Page 31 does not differentiate. Instead, it is up to the user to trouble shoot the failed communication. Thus, a window displayed indicating whether the tested remote system passed or failed. However, the "extraction" is based on a user selection of the remote system for testing and not based on whether the computer is present in said software-property management list and absent in said network-connected-computer list.

Furthermore, page 49 (section 7.3) clearly discloses that a message indicating that a host is unreachable is displayed when SafePatch is not detected (i.e., SafePatch is not detected or communicable with because the host is either not alive or because SafePatch is not installed and running on the host (page 31)). Again, the SafePatch Manual does not acknowledge what the root of the problem is, but instead notifies the user via message so that the user can troubleshoot. Thus, the message does not differentiate between a host that is not alive, a host that does not have SafePatch installed, or host that is not alive and that does not have SafePatch installed[2]. The SafePatch Manual simply does not disclose extracting a computer that is present in said software-property management list and absent in said network-connected-computer list. Also, the message in section 7.3 displayed indicating that SafePatch was not detected is not a list of

[2] For example, SafePatch permits a host to be added to a host list even if SafePatch is not running on the host or the host is not alive (page 4, paragraph 4).

computers in unused state (i.e., list of computers extracted) that are present in the software-property management list and absent in the network-connected-computer list.

Claim 17 recites that the computer not under software-property management includes a computer operating with an unknown operating system, software version, or patch-application status. The Examiner relies on page 34 for teaching the "unknown" operating system, software version, or patch-application. The Figure on page 34 relates to a report on an evaluated host or remote system. The Figure on page 34, however, clearly shows that the operating system , software version or patch-application **is known**. That is, for Server1 the operating system is clearly UNIX. Thus, it is known.

Claim 18 recites that the list of computer omitted in the software-property management includes information of the computer extracted. For reasons stated above, the SafePatch Manual fails to disclose extracting computers which are omitting in the software-property management. Computers in the result on pages 39-40 clearly are managed by SafePatch.

Claim 19 recites that the list of computer in unused state indicates a list of unused software. However, page 49 (section 7.3) merely discloses that a message indicating that a host is unreachable is displayed when SafePatch is not detected (i.e., SafePatch is not detected or communicable with because the host is either not alive or because SafePatch is not installed and running on the host (page 31)). Again, the SafePatch Manual does not acknowledge what the root of the problem is, but instead notifies the user via message so that the user can troubleshoot. Thus, the message does not differentiate between a host that is not alive, a host that does not have SafePatch installed, or host that is not alive and that does not have SafePatch installed[3]. The SafePatch Manual simply does not disclose extracting a computer that is present in said software-property management list and absent in said network-connected-computer list. Also, the message in section 7.3 displayed indicating that SafePatch was not detected is not a list of computers in unused state (i.e., list of computers extracted) that are present in the software-property management list and absent in the network-connected-computer list.

D. Remaining claims

The remaining claims should be patentable at least by virtue of their respective dependencies.

III. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

[3] For example, SafePatch permits a host to be added to a host list even if SafePatch is not running on the host or the host is not alive (page 4, paragraph 4).

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

Ryan F. Heavener
Registration No. 61,512

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: January 30, 2009